REMARKS

Applicants would like to thank the Examiner for the thorough examination of the present application, and for the courtesies extended during the telephone interview on March 19, 2008.

Based on the interview, the independent claims have been amended to more clearly define the present invention over the cited prior art references. The independent claims have been amended to highlight that the encoded output byte is for a cryptographic algorithm, and that generation of the bit string is based on an array of logic gates (instead of lookup tables). The claim amendments and arguments supporting patentability of the claims are provided below.

I. The Amended Claims

The present invention, as recited in amended independent Claim 12, for example, is directed to a method for generating output bytes corresponding to respective input bytes according to a one-to-one binary function representing a cryptographic algorithm. The method comprises decoding an input byte and generating at least one bit string that contains only one active bit, and using an array of logic gates for logically combining bits of the at least one bit string according to the one-to-one binary function and generating a 256-bit string without the use of a lookup table. The 256-bit string is encoded for obtaining an output byte for the cryptographic algorithm. The method advantageously allows for fast and low power hardware devices to be formed for generating output bytes corresponding to respective input bytes according to a one-to-one binary function. Such a one-to-one binary function is typically associated with an S-box

commonly used in cryptographic devices.

Amended independent Claim 17 is also directed to a method for generating output bytes, and has been amended similar to amended independent Claim 12, but does not recite the 256-bit string.

Amended independent Claim 23 is directed to a device for implementing a cryptographic algorithm, and has been amended similar to independent Claim 12.

Amended independent Claim 28 is directed to a cryptographic device, and has been amended similar to independent Claim 12.

II. The Amended Claims Are Patentable

The Examiner rejected independent Claims 12, 17, 23 and 28 over the Coppersmith et al. patent. The Coppersmith et al. patent is directed to a symmetric key cipher for encryption and decryption, using a block cipher algorithm. The Examiner has taken the position that Coppersmith et al. discloses the claimed invention.

As helpfully suggested by the Examiner during the telephone interview, the independent claims have been amended to highlight that the encoded output byte is for a cryptographic algorithm, and that generation of the 256-bit string is based on an array of logic gates (instead of lookup tables). In sharp contrast, the 256-bit string characterized by the Examiner in Coppersmith et al. is generated based on a lookup table. Reference is directed to column 3, lines 16-21 of Coppersmith et al., which provides:

> "The technique of the present invention achieves these objectives while using the simple operations of table lookup, exclusive

> OR, and key-dependent substitution, thereby minimizing the time required to encrypt and decrypt data." (Emphasis added).

In the claims of Coppersmith et al., a first substitution-box (S-box) lookup operation is recited, as well as a second substitution-box (S-box) lookup operation. The first and second S-box lookup operations are best illustrated in FIGS. 6 and 7.

Each of the two s-boxes is a one-dimensional array of non-repeating values between 0 and 255. The s-boxes each have 256 entries, so that indexing can be performed with an 8-bit number. Reference is directed to column 8, line 62 through column 9, line 4 of Coppersmith et al., which provides:

> "Each of the two s-boxes shown in FIG. 6 is a one-dimensional array of non-repeating values between 0 and 255, indexed from 0 to 255. (The s-boxes each have 256 entries, so that indexing can be performed with an 8-bit number, where 8 bits is the length of the value resulting from the two exclusive OR operations. Note that the values are shown in FIG. 6 using their decimal representation.) Referring again to the left-half mixing equation, it will be seen that when the byte counter i is an even number, s-box zero is used; when i is an odd number, s-box one is used." (Emphasis added).

In terms of logically combining bits of the at least one bit string according to the one-to-one binary function and generating a 256-bit string, the Examiner references the equation in column 8, line 16, where C represents a block of data. In terms of encoding the 256-bit string for obtaining an output byte, the Examiner references column 9, line 22 which states that the

functionality is provided by 2 boxes having 256 entries.

The Examiner further takes the position that access to the s-box array inherently expresses a 256-bit string whose active bit corresponds to an entry in the array. In terms of the encoding, the Examiner states that the 256-bit string is encoded to correspond to the actual substitution byte to be obtained.

In view of the amended independent claims, an array of logic gates is used for logically combining bits of the at least one bit string according to the one-to-one binary function and generating a 256-bit string without the use of a lookup table. The array of logic gates advantageously provides the function of an S-box without the use of lookup tables. In Coppersmith et al., output of the first and second S-boxes is based on lookup tables.

Accordingly, it is submitted that amended independent Claim 12 is patentable over the Coppersmith et al. patent. Amended independent Claims 17, 23 and 28 are similar to amended independent Claim 12. Therefore, it is submitted that these claims are also patentable over the Coppersmith et al. patent.

In view of the patentability of amended independent Claims 12, 17, 23 and 28, it is submitted that their dependent claims, which recite yet further distinguishing features of the invention, are also patentable. These dependent claims require no further discussion herein.

III. CONCLUSION

In view of the claim amendments and arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner

is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330